## REMARKS

Reconsideration of the application is respectfully requested for the following reasons:

1. Formalities

The claims, specification, and abstract have been revised to place the application in proper U.S. format, including the addition of headers to the specification, and deletion of "and/or" and "preferably" phraseology from the claims.

Because the changes are all formal in nature, it is respectfully submitted that the changes do not involve new matter.

2. Rejection of Claims 6-10 and 17-19 Under 35 USC §112, 2nd Paragraph

This rejection has been addressed by amending claim 9 to depend from claim 8, and to clarify that the "calculation" in question is the calculation of the authentication parameters recited in claim 8.

3. Rejection of Claims 1-3 and 5-11 Under 35 USC §103(a) in view of U.S. Patent No. 6,049,611 (Tatebayashi) and "*Applied Cryptography*" (Schneier)

This rejection is respectfully traversed on the grounds that neither the Tatebayashi patent nor the Schneier article discloses or suggests, whether considered individually or in any reasonable combination, a smart card authentication method in which a secret key stored in the smart card is split into two, the resulting split keys being used to encrypt a split random number transmitted to the smart card by the authenticating network as claimed.

The Tatebayashi patent discloses an authentication system in which a random number is transmitted, as in the claimed invention, from the authenticating site (corresponding to the claimed network) to the site to be authenticated (corresponding to the smart card of the claimed invention), and in which the random number is then used to generate a response signal.

Furthermore, as disclosed in col. 7, lines 7-19 of the Tatebayashi patent, the random number is split by a hard wired separator unit 52 in the authenticating site. However, the Tatebayashi patent does not disclose or suggest splitting a secret key stored in the site to be authenticated in the claimed manner.

According to the Examiner, the feature of splitting the secret key is suggested by the Schneier article. However, in the Schneier article, the only key "splitting" is generation of a **48-bit "subkey"** by ignoring 8 bits of a 56-bit key, as part of the DES encryption process (actually, the original key is 64-bits, but 8 bits are parity bits that are ignored encoding). During the encryption process, 28-bit keys are formed and essentially shuffled around before being re-combined. To the extent that this can even be characterized as key splitting, the key splitting of Schneier is carried out as part of an encryption process in which a 56-bit key is split and shifted, *and then used to **reconstitute** a 48 bit key.* The method of Schneier does not result in the generation of generation of two encryption keys by splitting one key, but rather involves shuffling and discarding bits of a 56-bit key to obtain a 48-bit key. This has nothing to do with the encryption of a split random number of the type taught by Tatebayashi, or the key splitting of the claimed invention, and the split 28-bit keys of Schneier cannot be used for the purposes of the claimed invention.

The 28-bit split key halves of Schneier are never used by themselves as encryption keys. In contrast, in the claimed method, the key is split **before** use in an encryption algorithm, with one of the split parts of the key actually being used to encrypt one of the split parts of the random number. This feature is specifically recited in claim 1, as follows:

> *. . .one of the parts ($RAND_1$, $RAND_2$) of the transferred random number (RAND) is encrypted with the aid of one or more parts ($K_1$, $K_2$) of the secret key ($K_i$) by means of a one- or multistep algorithm.*

Because Schneier fails to disclose use of the split secret key to encrypt a previously split number, thereby preventing simulation of essential functional elements of the card being authenticated, and because Tatebayashi fails to disclose *any* secret key splitting, withdrawal of the rejection of claims 1-3 and 5-11 under 35 USC §103(a) is respectfully requested.

4. Rejection of Claims 4 Under 35 USC §103(a) in view of U.S. Patent No. 6,049,611 (Tatebayashi), "*Applied Cryptography*" (Schneier), and U.S. Patent No. 5,537,474 (Brown)

This rejection is respectfully traversed on the grounds that the Brown patent, like the Tatebayashi patent and the Schneier article, fails to disclose or suggest, whether considered individually or in any reasonable combination, the claimed smart card authentication method in which a secret key stored in the smart card is split into two, the resulting split keys being used to encrypt a split random number transmitted to the smart card by the authenticating network.

Instead, the Brown patent teaches the random number challenge recited in the preamble of claim 1. The random number of Brown is not split, and not encrypted by keys split from the secret key stored on the smart card. Therefore, the Brown patent could not possibly have suggested modification of the authentication method of Tatebayashi, considered in view of Schneier, to encrypt split random numbers by a split secret key, as claimed, and withdrawal of the rejection of claim 4 under 35 USC §103(a) is respectfully requested.

Having thus overcome each of the rejections made in the Official Action, withdrawal of the rejections and expedited passage of the application to issue is requested.

Respectfully submitted,

BACON & THOMAS, PLLC

By: BENJAMIN E. URCIA
Registration No. 33,805

Date: June 29, 2004

BACON & THOMAS, PLLC
625 Slaters Lane, 4th Floor
Alexandria, Virginia 22314
Telephone: (703) 683-0500

NWB:S:\Prosecution\Pending Q. Z:\VVEDDER 67365\RA01.wpd